

中国密码学会

关于全国密码算法设计竞赛算法评选结果的公示

根据全国密码算法设计竞赛的工作安排，经形式审查、公开评议、检测评估和专家评选，竞赛最终评选结果已经揭晓。现将《全国密码算法设计竞赛公钥算法评选结果》（见附件1）和《全国密码算法设计竞赛分组算法评选结果》（见附件2）予以公示，任何单位和个人如对公示的评选结果持有异议，请在公示之日起5天内向中国密码学会办公室提出。提出异议的单位或个人，应以真实身份书面形式提出申诉理由和意见，并附上有关证明材料及联系方式，否则不予受理。

联系电话：010-59703621

地 址：北京市丰台区靛厂路7号(100036)

邮 箱：cacr@cacrnet.org.cn

- 附件：1. 全国密码算法设计竞赛公钥算法评选结果
2. 全国密码算法设计竞赛分组算法评选结果



附件 1

全国密码算法设计竞赛公钥算法评选结果

一等奖: Aigis-sig、LAC.PKE、 Aigis-enc

二等奖: LAC.KEX、SIAKE、SCloud、AKCN(原名
AKCN-MLWE)

三等奖: OKCN(原名 SKCN-MLWE)、Fatseal、木兰、
AKCN-E8、TALE、PKP-DSS、Piglet-1

China Cryptographic Society

Announcement of the results of the national cryptographic algorithm design competition algorithm selection

According to the work arrangement of the National Cryptographic Algorithm Design Competition, after formal review, Public review, testing and evaluation, and expert selection, the final selection results of the competition have been revealed dawn. The "National Cryptographic Algorithm Design Competition Public Key Algorithm Selection Results" (see Attachment 1) and "Selection Results of Grouping Algorithms in the National Encryption Algorithm Design Competition" (see Attachment 2) To be publicized, any unit or individual who holds the opinion of the publicized selection results If you have any objections, please submit it to the Office of the Chinese Cryptography Society within 5 days from the date of publication. The unit or individual that raises the objection shall submit the complaint in written form with their true identity. Opinions and relevant supporting materials and contact information are attached, otherwise it will not be accepted.

Contact number: 01. "59703621

land Address: No. 7 Kengchang Road, Fengtai District, Beijing (100036)

Email: cacr@cacnet.org.cn

Attachment: 1. Public key algorithm selection results of the National Cryptographic Algorithm Design Competition
2. Selection results of grouping algorithms in the National Encryption Algorithm Design Competition

attachment1

Public Key Algorithm Selection Results of the National Cryptographic Algorithm Design Competition

First prize: Aigis-sig, LAC.PKE, Aigis-enc

Second prize: LAC.KEX, SIAKE, SCloud, AKCN (formerly

AKCN-MLWE)

Third prize: OKCN (formerly known as SKCN-Zhou WE), Fatseal, Mulan,

AKCN-E8, TALE, PKP-DSS, Piglet- I